Claims

We claim:

1 A method for secure distribution of digital content to an untrusted environment, comprising the steps of:

constructing a relatively trusted environment within said untrusted environment;

constructing at least two digital inputs, said digital inputs are operable in order to reproduce said digital content;

transferring digital media to said relatively trusted environment such that each of said inputs is transmitted via a different path, and

combining said inputs in order to reproduce said digital content.

2 A method according to claim 1 wherein said digital content is a document.

3 A method according to claim 2 wherein said digital content is multimedia digital content.

4 A method according to claim 3 wherein said multimedia digital content is an audio digital content.

5 A method according to claim 3 wherein said multimedia digital content is a video digital content.

6 A method according to claim 3 wherein said multimedia digital content consists of at least two different streams.

7 A method according to claim 6 wherein at least one of said different streams consists of video digital content.

8 A method according to claim 6 wherein at least one of said different

streams consists of audio digital content.

9 A method according to claim 6 wherein at least one of said different streams consists of textual digital content.

10 A method according to claim 1 wherein said untrusted environment comprise a consumer's computer.

11 A method according to claim 1 wherein said relatively trusted environment comprise a software component.

12 A method according to claim 11 wherein said software component is updateable.

13 A method according to claim 11 wherein said software component comprise at least one tamper resistant software component.

14 A method according to claim 13 wherein at least one of said software components is updateable.

15 A method according to claim 1 wherein said relatively trusted environment comprise a hardware component.

16 A method according to claim 15 wherein said hardware component comprise at least one tamper resistant hardware component.

17 A method according to claim 1 wherein said relatively trusted environment comprise a firmware component.

18 A method according to claim 17 wherein said firmware component is updateable.

19 A method according to claim 17 wherein said firmware component comprise at least one tamper resistant firmware component.

20 A method according to claim 19 wherein at least one of said tamper resistant firmware components is updateable.

21 A method according to claim 1 wherein said relatively trusted environment comprise at least two components.

22 A method according to claim 21 wherein at least one of said components comprises a software component.

23 A method according to claim 22 wherein said software component is updateable.

24 A method according to claim 22 wherein said software component comprise at least one tamper resistant software component.

25 A method according to claim 24 wherein at least one of said software components is updateable.

26 A method according to claim 21 wherein at least one of said components comprises a hardware component.

27 A method according to claim 26 wherein said hardware component comprise at least one tamper resistant hardware component.

28 A method according to claim 21 wherein at least one of said components comprises a firmware component.

29 A method according to claim 28 wherein said software firmware is updateable.

30 A method according to claim 28 wherein said firmware component comprise at least one tamper resistant firmware component.

31 A method according to claim 30 wherein at least one of said firmware

components is updateable.

32 A method according to claim 1 wherein at least one of said inputs comprise of a key.

33 A method according to claim 32 wherein said key is a cryptographic key.

34 A method according to claim 32 wherein said key is a scrambling key.

35 A method according to claim 1 wherein at least one of said inputs comprise of a scrambled copy of said digital content, and at least one other input comprise of the information needed for said reproduction.

36 A method according to claim 1 wherein a group of at least two of said inputs comprise of a function of a scrambled copy of said digital content, and at least one other input comprise of the information needed for reconstruction.

37 A method according to claim 1 wherein said reproduction results in an output which is identical to said digital content.

38 A method according to claim 1 wherein said reproduction results in an output which is sufficiently similar to said digital content.

39 A method according to claim 1 wherein a group of at least two of said inputs comprises of a function of said digital content.

40 A method according to claim 39 wherein said function comprises of splitting said digital content to said inputs.

41 A method according to claim 1 wherein said method comprise of using at least one updateable component.

42 A method according to claim 41 wherein said updateable component is associated with a revision level identifier.

43 A method according to claim 42 wherein said revision level identifier is a version number.

44 A method according to claim 42 wherein said revision level identifier is revision date.

45 A method according to claim 42 wherein at least one aspect of operation of the underlying system depends on said revision level.

46 A method according to claim 45 wherein at least some functionality of the underlying system is limited if said revision level does not belong to a specific set of revision levels.

47 A method according to claim 46 wherein said limited functionality comprise of the ability to receive a set of digital content.

48 A method according to claim 46 wherein said limited functionality comprise of the ability to receive a set of digital content in a specific format.

49 A method according to claim 46 wherein said limited functionality comprise of the ability to receive a set of digital content in a specific method.

50 A method according to claim 42 wherein said revision level is communicated to at least one other component of the underlying system by said updateable component.

51 A method according to claim 50 wherein said communication is initiated by said updateable component.

52 A method according to claim 50 wherein said communication is part of another communication that is part of the normal workflow of the underlying system.

53 A method according to claim 50 wherein said communication is initiated by said other component of the underlying system.

54 A method according to claim 41 wherein a component within said untrusted environment queries another component in the underlying system for revisioned version of said updateable component.

55 A method according to claim 41 wherein transfer of said updateable component is performed automatically without intervention.

56 A method according to claim 41 wherein transfer of said updateable component is initiated by approval.

57 A method according to claim 41 wherein installation of said updateable component is performed automatically without intervention.

58 A method according to claim 41 wherein installation of said updateable component is initiated by approval.

59 A method according to claim 1 wherein said digital content is split into said separate inputs in a relatively trusted server, said server is operable to deliver said digital content to said relatively trusted environment in the form of said separate inputs

60 A method according to claim 59 wherein said digital content arrives in the form of second separate inputs different from said first separate inputs to said relatively trusted server, said relatively trusted server is operable to rearrange said digital content to the form of said first separate inputs

61 A method according to claim 1 wherein said digital content arrives in the form of said separate inputs to a server, said server is operable to

deliver said digital content to said relatively trusted environment in the form of said separate inputs

62 A method for secure distribution of digital content comprising the steps of:

gathering input from at least one source;

producing trustworthiness credentials about said digital content's intended recipient environment based on said input;

evaluate said intended recipient environment's trustworthiness credentials;

determine a distribution policy according to said trustworthiness credentials evaluation, and

performing decisions about said distribution according to said policy.

63 A method according to claim 62 wherein said digital content is a document.

64 A method according to claim 62 wherein said digital content is multimedia digital content.

65 A method according to claim 64 wherein said multimedia digital content is an audio digital content.

66 A method according to claim 64 wherein said multimedia digital content is a video digital content.

67 A method according to claim 64 wherein said multimedia digital content consists of at least two different streams.

68 A method according to claim 62 wherein said credentials comprise geo-location information.

69 A method according to claim 62 wherein said credentials comprise geo-location authentication level information.

70 A method according to claim 62 wherein said credentials comprise authentication level information.

71 A method according to claim 62 wherein said credentials comprise information gathered in the past.

72 A method according to claim 71 wherein said credentials further comprise information gathered from analysis of said information gathered in the past.

73 A method according to claim 71 wherein said information gathered in the past comprise of usage information.

74 A method according to claim 62 wherein said credentials comprise of information about the environment into which said digital content is to be distributed.

75 A method according to claim 74 wherein said information about the environment into which said digital content is to be distributed comprise of information about the software environment into which said digital content is to be distributed.

76 A method according to claim 74 wherein said information about the environment into which said digital content is to be distributed comprise of information about the hardware environment into which said digital content is to be distributed.

77 A method according to claim 76 wherein said information about the hardware environment into which said digital content is to be distributed comprise information about the video output hardware in that environment.

78 A method according to claim 76 wherein said information about the hardware environment into which said digital content is to be distributed comprise information about the sound output hardware in that environment.

79 A method according to claim 74 wherein said information about the environment into which said digital content is to be distributed comprise of information about the firmware environment into which said digital content is to be distributed.

80 A method according to claim 62 wherein said credentials comprise of reports from at least one relatively trusted component.

81 A method according to claim 80 wherein at least one of said components reside in the consumer's computer.

82 A method according to claim 80 wherein at least one of said components is connected to the consumer's computer.

83 A method according to claim 80 wherein at least one of said components is a software component.

84 A method according to claim 80 wherein at least one of said components is a firmware component.

85 A method according to claim 80 wherein at least one of said components is a tamper resistant component.

86 A method according to claim 80 wherein at least one of said components

is a hardware component.

87 A method according to claim 83 wherein at least one of said software components is updateable.

88 A method according to claim 84 wherein at least one of said firmware components is updateable.

89 A method according to claim 62 wherein said method comprise of using at least one updateable component.

90 A method according to claim 89 wherein said updateable component is associated with a revision level identifier.

91 A method according to claim 90 wherein said revision level identifier is a version number.

92 A method according to claim 90 wherein said revision level identifier is revision date.

93 A method according to claim 90 wherein at least one aspect of operation of the underlying system depends on said revision level.

94 A method according to claim 93 wherein at least some functionality of the underlying system is limited if said revision level does not belong to a specific set of revision levels.

95 A method according to claim 94 wherein said limited functionality comprise of the ability to receive a set of digital content.

96 A method according to claim 94 wherein said limited functionality comprise of the ability to receive a set of digital content in a specific format.

97 A method according to claim 94 wherein said limited functionality

comprise of the ability to receive a set of digital content in a specific method.

98 A method according to claim 90 wherein said revision level is communicated to at least one other component of the underlying system by said updateable component.

99 A method according to claim 98 wherein said communication is initiated by said updateable component.

100 A method according to claim 98 wherein said communication is part of another communication that is part of the normal workflow of the underlying system.

101 A method according to claim 98 wherein said communication is initiated by said other component of the underlying system.

102 A method according to claim 89 wherein a component within said untrusted environment queries another component in the underlying system for revisioned version of said updateable component.

103 A method according to claim 89 wherein transfer of said updateable component is performed automatically without intervention.

104 A method according to claim 89 wherein transfer of said updateable component is initiated by approval.

105 A method according to claim 89 wherein installation of said updateable component is performed automatically without intervention.

106 A method according to claim 89 wherein installation of said updateable component is initiated by approval.

107 A method according to claim 89 wherein said credentials

comprise of said revision level.

108 A method for secure distribution of digital content comprising the steps of:

transferring digital media to an untrusted environment;

using a relatively trusted environment within said untrusted environment operable to receive said digital content, said relatively trusted environment comprises of mechanisms to restrict tampering with said relatively trusted environment.

109 A method according to claim 108 wherein said relatively trusted environment comprise at least two components.

110 A method according to claim 109 wherein said components comprise at least one hardware component.

111 A method according to claim 109 wherein said components comprise at least one software component.

112 A method according to claim 109 wherein said components comprise at least one firmware component.

113 A method according to claim 108 wherein said relatively trusted environment is a hardware component.

114 A method according to claim 108 wherein said relatively trusted environment is a firmware component.

115 A method according to claim 108 wherein said relatively trusted environment is a software component.

116 A method according to claim 109 wherein said components comprise a watchdog component, wherein said watchdog component is capable of monitoring other components of the relatively trusted environment.

117 A method according to claim 116 wherein said monitoring comprise of authentication.

118 A method according to claim 117 wherein said authentication comprise authentication of a certificate.

119 A method according to claim 118 wherein said certificate is a cryptographic certificate.

120 A method according to claim 117 wherein said authentication comprise authentication of the code of the component.

121 A method according to claim 120 wherein said authentication of the code of the component comprises calculating a derivative of said code.

122 A method according to claim 120 wherein said authentication of the code of the component comprises analysis of the potential operation of said code.

123 A method according to claim 117 wherein said authentication comprise of a challenge-response method which comprise of a step in which said watchdog component queries the authenticated component issuing a input and further comprises of a later step in which the authenticated component issue an output to the watchdog said output dependent on said input and said authentication is based on the correctness of said output depending on said input.

124 A method according to claim 116 wherein said monitoring comprises monitoring of the operation of said components.

125 A method according to claim 124 wherein said monitoring of the operation of said components comprise monitoring of used interfaces.

126 A method according to claim 125 wherein said monitoring of used interfaces comprise monitoring of used operating system calls.

127 A method according to claim 125 wherein said monitoring of used interfaces comprise monitoring of file operations.

128 A method according to claim 125 wherein said monitoring of used interfaces comprise monitoring of memory operations.

129 A method according to claim 125 wherein said monitoring of used interfaces comprise monitoring of communication operations.

130 A method according to claim 125 wherein said monitoring of used interfaces comprise monitoring of driver operations.

131 A method according to claim 125 wherein said monitoring of used interfaces comprise monitoring of input operations

132 A method according to claim 125 wherein said monitoring of used interfaces comprise monitoring of output operations

133 A method according to claim 125 wherein said monitoring of used interfaces comprise monitoring of interfaces used by interfaced entities.

134 A method according to claim 108 wherein said relatively trusted environment comprise at least one updateable component.

135 A method according to claim 134 wherein said updateable component is associated with a revision level identifier.

136 A method according to claim 135 wherein said revision level identifier is

a version number.

137 A method according to claim 135 wherein said revision level identifier is revision date.

138 A method according to claim 135 wherein at least one aspect of operation of the underlying system depends on said revision level.

139 A method according to claim 138 wherein at least some functionality of the underlying system is limited if said revision level does not belong to a specific set of revision levels.

140 A method according to claim 139 wherein said limited functionality comprise of the ability to receive a set of digital content.

141 A method according to claim 139 wherein said limited functionality comprise of the ability to receive a set of digital content in a specific format.

142 A method according to claim 139 wherein said limited functionality comprise of the ability to receive a set of digital content in a specific method.

143 A method according to claim 135 wherein said revision level is communicated to at least one other component of the underlying system by said updateable component.

144 A method according to claim 143 wherein said communication is initiated by said updateable component.

145 A method according to claim 143 wherein said communication is part of another communication that is part of the normal workflow of the underlying system.

146 A method according to claim 143 wherein said communication is initiated

by said other component of the underlying system.

147 A method according to claim 134 wherein a component within said untrusted environment queries another component in the underlying system for revisioned version of said updateable component.

148 A method according to claim 134 wherein transfer of said updateable component is performed automatically without intervention.

149 A method according to claim 134 wherein transfer of said updateable component is initiated by approval.

150 A method according to claim 134 wherein installation of said updateable component is performed automatically without intervention.

151 A method according to claim 134 wherein installation of said updateable component is initiated by approval.

152 A method according to claim 109 wherein at least one of said components comprise of functionality to monitor at least one of its interfaces.

153 A method according to claim 152 wherein said monitoring comprise of authentication.

154 A method according to claim 153 wherein said authentication comprise authentication of a certificate.

155 A method according to claim 154 wherein said certificate is a cryptographic certificate.

156 A method according to claim 153 wherein said authentication comprise of a challenge-response method which comprise of a step in which said component queries the interfaced entity issuing a input and further comprises

of a later step in which the interfaced entity issue an output to said component said output dependent on said input and said authentication is based on the correctness of said output depending on said input.

157 A method according to claim 108 wherein said method comprises of functionality to monitor at least one of the interfaces used by the underlying system.

158 A method according to claim 157 wherein said monitoring comprise of authentication.

159 A method according to claim 158 wherein said authentication comprise authentication of a certificate.

160 A method according to claim 159 wherein said certificate is a cryptographic certificate.

161 A method according to claim 158 wherein said authentication comprise of a challenge-response method which comprise of a step in which the interfaced entity is queried by issuing a input and further comprises of a later step in which the interfaced entity issue back an output said output dependent on said input and said authentication is based on the correctness of said output depending on said input.

162 A method according to claim 108 wherein said digital content arrives into said relatively trusted environment in a cryptographically encrypted format.

163 A method according to claim 116 wherein information gathered from monitoring by at least one component is transferred to said watchdog component by said component.

164 A method according to claim 163 wherein information gathered by said watchdog component is transferred as credentials information to a credentials based decision making mechanism.

165 A method according to claim 116 wherein information gathered by said watchdog component is transferred as credentials information to a credentials based decision making mechanism.

166 A method according to claim 108 wherein said relatively trusted environment comprise mechanism to restrict coping of at least one of the outputs said relatively trusted environment generates.

167 A method according to claim 166 wherein said output is part of an internal interface.

168 A method according to claim 166 wherein said output is an external output.

169 A method according to claim 168 wherein said external output is sound output.

170 A method according to claim 168 wherein said external output is video output.

171 A method according to claim 168 wherein said external output is analog output.

172 A method according to claim 171 wherein said analog output is analog sound output.

173 A method according to claim 171 wherein said analog output is analog video output.

174 A method according to claim 166 wherein said mechanism to restrict coping comprise of altering the output in order to change a quality of the copy which is produced by said copying.

175 A method according to claim 174 wherein said quality of said copy is the observable quality of the copy.

176 A method according to claim 174 wherein said change of said quality is to adversely effect said quality.

177 A method according to claim 174 wherein said copying is digital copying.

178 A method according to claim 174 wherein said copying is non-digital copying.

179 A method according to claim 174 wherein said copying is digital copying which involves a non-digital transition.